代號：01340
頁次：1－1

107年專門職業及技術人員高等考試
建築師、技師、第二次食品技師考試暨
普通考試不動產經紀人、記帳士考試試題

等　　別：高等考試
類　　科：資訊技師
科　　目：系統分析與資訊安全
考試時間：2小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、請說明何謂類別（Class），類別如同物件般由那三項特性（那三部分）構成？又何謂組合類別？並舉例畫圖說明之。（30分）

二、物件導向之抽象類別（Abstract Class）是一種不能實體化的類別，其抽象方法（Abstract Method）則只定義規格卻沒有實作的方法，因此抽象類別使用時機為需要定義規格供其他類別使用時。請問其實作方式需透過物件導向的那一種特性讓前來實作的類別擁有相同的規格？使用何種操作方法來操作物件以方便維護與擴充程式？（20分）

三、Ron Rivest、Adi Shamir 與 Len Adleman 於 1978 年發表了 Rivest－Shamir－Adleman（RSA）公開金鑰演算法如下：
密文＝$(\text{原文})^{e} \bmod n$
原文＝$(\text{密文})^{d} \bmod n$
私密金鑰＝{d,n}
公開金鑰＝{e,n}
其中 mod 表示除餘，RSA 可以逆向操作確認資訊的來源。
假設知道私密金鑰＝{d,n}，公開金鑰＝{e,n}，則密文與原文的演算法各為何？（20分）

四、防火牆（Firewall）基本上可以分為那兩類型？使用代理器控制網路連線的是那一種防火牆？除了檢查規則設定外還會藉由網路連線的狀態判斷是否允許封包通過的是那一種防火牆？（30分）